UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/750,340	12/31/2003	Selim Aissi	884.B30US1	4702

21186 7590 05/16/2007

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
P.O. BOX 2938
MINNEAPOLIS, MN 55402

EXAMINER	
LEMMA, SAMSON B	

ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
05/16/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/750,340	AISSI ET AL.	
	Examiner	Art Unit	
	Samson B. Lemma	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 December 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5,8-10 and 16-33* is/are rejected.

7)☒ Claim(s) *6-7 and 11-15* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *12/02/05*.
4) ☐ Interview Summary (PTO-413). Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. **Claims 1-33** have been examined.

Priority

2. This application does not claim priority. Therefore, the effective filling data for the subject matter defined in the pending claims of this application is **12/31/2003.**

Claim Rejections - 35 USC § 101

3. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4. **Claims 25-33** are rejected under 35 U.S.C. 101 because the subject matter is directed to non-statutory subject matter.

5. **Claims 25-33** recites a machine-readable medium that provides instructions when executed by a machine, cause said machine to perform operations. On applicant's disclosure, **on page 35, lines 27-29** or **on paragraph "0128" of the publication** the following has been recited. "In an exemplary embodiment, a machine-readable medium includes **electrical, optical, acoustical or other form of propagated signals (e.g., carrier waves, infrared signals, digital signals, etc."**

Such storage medium/machine-readable medium is considered non-statutory.

Examiner asserts that in view of the specification, the limitation of the claims does not fall within the statutory classes listed in 35 USC 101. The language of the claims raises a question as to whether the claims are directed merely to an

abstract idea/storage medium which could be a signal that is not tied to a technological art, environment or machine which would result in a practical application producing a concrete, useful, and tangible result to form the basis of statutory subject matter under 35 U.S.C. 101.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. **Claims 1, 4-5, 8-10, 16-18 and 21-33** are rejected under 35 U.S.C. 102(e) as being anticipated by **Trostle** (hereinafter referred to as **Trostle**) (U.S. Patent No. 6,718,467 B1) (filed on October 28, 1999)

8. **As per Independent claims 1, 8, 16, 21, 25, 28 and 31 Trostle discloses a method comprising:**

Performing an authentication *[Figure1 and figure 3]* **of a computing device** *[figure 1, ref. Num "100"/client]* **and equipment of an operator of services for the**

computing device *[figure 1, ref. Num "102"/SERVER]* **for a session of communication between the computing device and the equipment,** *[figure 1, ref. "104", "106", "108" and "110" or see also figure 3]* **the performing comprising:**

- **Generating, in the computing device** [figure 1, ref. Num "100"/client], **a random number;** *[column 5, lines 34-35 and figure 1, ref. Num "104", see "c"] (On column 5, lines 34-35 and on figure 1, ref. Num "104", c the following has been disclosed. "Additionally, C/Client 100 generates random values for authenticators c and s.")*

- **Generating a one-time-pad key based on a hash operation of a value** *[Column 5, lines 31-33, "$DHKey_1$" or K which is the hash of encryption key k see column 4, lines 50-51]* **based on operation of a value selected from the group consisting of an identification of the computing device** *[$DHkey_1=Y_1^{x1}$ mod p, notice that x1 the private Diffie-Hellman values of the computer device or the client or K/one-time-pad key is the hash value of the secret password]* **an identification of the equipment** *[$DHkey_1=Y_1^{x1}$ mod p, notice that Y1 the public Diffie-Hellman values of the equipment/server]* **,stored in a protected storage within the computing device** *[See Table 2 and column 5, lines 1-2, "Both the client/computing device 100 and the server/Equipment102 store the current shared private key] (Furthermore see column 5, lines 20-35] and*

- **Encrypting the random number based on the one-time-pad key** *[See figure 1, ref. Num "104" and column 5, lines 42-44, "while y1 and s are encrypted with K and the hashed value of c is encrypted with $DHkey_1$"];*

- **Transmitting the encrypted random number to the equipment** *[See figure 1, ref. Num "104" and column 5, lines 35-38, "client/c/ computing device 100 sends the msg 104 to the Server 102/equipment];*

- **Receiving, from the equipment [Figure 1, ref. Num "102"], an encrypted value [column 5, lines 54-58] in response to the encrypted random number, wherein the encrypted value includes a challenge of a challenge-response** *(See on figure 1, ref. Num, "106" or see also on column 5, lines 54-58, msg 106 notice that [s, Y_2] is encrypted by $DHkey_1$ And THIS IS SEND FROM THE SERVER 102/EQIPMENT AND SEND TO THE CLIENT/COMPUTING DEVICE, INOTHER WORDS IT IS RECIVED FROM THE EQUIPMENT/SEVER 102);*

- **Verifying the encrypted value [Column 5, lines 60-65)** *(When C/client or computing device 100 receives message 106, C, it decrypts message 106 to obtain s and Y.sub.2. C 100 uses s in message 106 to authenticate S. Specifically, C 100 compares the value of s sent in message 104 with the value of s decrypted in message 106. If the two values are the same, C 100 knows that S 102 sent the message, since only C 100 and S 102 know K);*

- **Encrypting a response to the challenge of the challenge-response ; transmitting the response to the equipment** [See figure 1, ref. Num "108" and column 6, lines 17-19,see msg "108"]; **and receiving, from the equipment, an authentication verification** [figure 1, ref. Num "110", column 6, lines 23-35] .

9. **<u>As per claims 4-5, 9-10, 17-18, 22-24, 26-27, 29-30 and 32-33</u> Trostle discloses a method as applied to the claims above. Furthermore, Trostle discloses the**, wherein the challenge of the challenge-response comprises an encryption of a data string that includes a concatenation of the random number generated in the computing device, a random number generated by the equipment and the identification of the session. [See figure 1 and column 3, lines 55-67, table 1]

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. **Claims 2-3 and 19-20** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Trostle** (hereinafter referred to as **Trostle**) (U.S. Patent No. 6,718,467 B1) (filed on October 28, 1999) in view of **Mitchell et al** (hereinafter referred to as **Mitchell) (Patent No.** 6950522)

12. **As per claims 2-3 and 19-20 Trostle discloses a method comprising:**

Performing an authentication *[Figure1 and figure 3]* **of a computing device** *[figure 1, ref. Num "100"/client]* **and equipment of an operator of services for the computing device** *[figure 1, ref. Num "102"/SERVER]* **for a session of communication between the computing device and the equipment,** *[figure 1, ref. "104", "106", "108" and "110" or see also figure 3]* **the performing comprising:**

- **Generating, in the computing device** [figure 1, ref. Num "100"/client], **a random number;** *[column 5, lines 34-35 and figure 1, ref. Num "104", see "c"] (On column 5, lines 34-35 and on figure 1, ref. Num "104", c the following has been disclosed. "Additionally, C/Client 100 generates random values for authenticators c and s.")*

- **Generating a one-time-pad key based on a hash operation of a value** *[Column 5, lines 31-33, "DHKey$_1$" or K which is the hash of encryption key k see column 4, lines 50-51]* **based on operation of a value selected from the group consisting of an identification of the computing device** *[DHkey$_1$=Y$_1^{x1}$ mod p, notice that x1 the*

private Diffie-Hellman values of the computer device or the client or K/one-time-pad key is the hash value of the secret password] **an identification of the equipment** *[DHkey$_1$=Y_1^{x1} mod p, notice that Y1 the public Diffie-Hellman values of the equipment/server]* **,stored in a protected storage within the computing device** *[See Table 2 and column 5, lines 1-2, "Both the client/computing device 100 and the server/Equipment102 store the current shared private key] (Furthermore see column 5, lines 20-35] and*

- **Encrypting the random number based on the one-time-pad key** *[See figure 1, ref. Num "104" and column 5, lines 42-44, "while y1 and s are encrypted with K and the hashed value of c is encrypted with DHkey$_1$"];*

- **Transmitting the encrypted random number to the equipment** *[See figure 1, ref. Num "104" and column 5, lines 35-38, "client/c/ computing device 100 sends the msg 104 to the Server 102/equipment];*

- **Receiving, from the equipment [Figure 1, ref. Num "102"], an encrypted value [column 5, lines 54-58] in response to the encrypted random number, wherein the encrypted value includes a challenge of a challenge-response** *(See on figure 1, ref. Num, "106" or see also on column 5, lines 54-58, msg 106 notice that [s, Y_2] is encrypted by DHkey$_1$ And THIS IS SEND FROM THE SERVER 102/EQIPMENT AND SEND TO THE CLIENT/COMPUTING DEVICE, INOTHER WORDS IT IS RECIVED FROM THE EQUIPMENT/SEVER 102);*

- **Verifying the encrypted value [Column 5, lines 60-65)** *(When C/client or computing device 100 receives message 106, C, it decrypts message 106 to obtain s and Y.sub.2. C 100 uses s in message 106 to authenticate S. Specifically, C 100 compares the value of s sent in message 104 with the value of s decrypted in message*

106. If the two values are the same, C 100 knows that S 102 sent the message, since only C 100 and S 102 know K);

- **Encrypting a response to the challenge of the challenge-response ; transmitting the response to the equipment** [See figure 1, ref. Num "108" and column 6, lines 17-19,see msg "108"]; **and receiving, from the equipment, an authentication verification** [figure 1, ref. Num "110", column 6, lines 23-35] .

Trostle does not explicitly disclose

One time encrypting key is based on the platform configuration measurement of the computing device comprises a version of hardware/software in the computing device

However, in the same field of **Mitchell**, discloses the generation of the key for that site with a one digit Hex **version tag** or number of "1". [See column 6, lines 47-48] Furthermore **Mitchell** discloses the feature that a version number could be associated with an encrypted key executable to allow real time updating of keys for a system which facilitates users signing on to multiple websites on different domains using an encrypted ticket which meets the limitation of generating encrypting key based on the version number. [See Abstract]

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the feature of version number as per teachings of **Mitchell**, into the method as taught by **Trostle** in order provide real time updating of keys. [*See Abstract]*

Allowable Subject Matter

13. **Claims 6-7 and 11-15 are objected** to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

14. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.(See PTO-Form 892).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571 -873-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA
SL.
05/01/2007

Benjamin E. Lanier
Examiner AU 2182